CLAIMS

WHAT IS CLAIMED IS:

1. A system, comprising:

a crypto-processor; and

a memory coupled to receive memory transactions through the crypto-processor, wherein the memory transactions are passed to the memory by the crypto-processor.

2. The system of claim 1, wherein the crypto-processor includes a memory permission table that maps at least a portion of the memory; and wherein the crypto-processor is configured to pass the memory transactions to the memory if the memory access is indicated as allowed by the memory permission table.

3. The system of claim 2, wherein the crypto-processor is configured to pass the memory transactions to the memory only if the memory access is indicated as allowed by the memory permission table.

4. The system of claim 1, further comprising:

a device different from the crypto-processor, wherein the device is configured to request the memory transactions passed to the memory by the crypto-processor.

5. The system of claim 1, further comprising:

a bridge;

a first bus coupled between the device and the bridge; and

a second bus coupled between the bridge and the crypto-processor.

6. The system of claim 1, wherein the crypto-processor includes a secret; and wherein the crypto-processor is configured to demand an authorization before passing the memory access to the memory, wherein the authorization comprises an indication from the device of the secret.

7. The system of claim 6, wherein the indication of the secret comprises a correct response to a challenge-response authentication.

8. The system of claim 1, wherein the memory comprises a ROM.

9. The system of claim 8, wherein the ROM comprises a BIOS ROM.

10. The system of claim 1, wherein the memory comprises a flash memory.

11. The system of claim 1, wherein the crypto-processor and the memory are integrated into a protected storage device, the protected storage device comprising:

one or more storage areas;

logic for controlling access to the one or more storage areas;

a random number generator; and

a secret.

12. The system of claim 11, wherein the one or more storage areas comprises a data storage and a code storage.

13. The system of claim 12, wherein the secret is comprised within the code storage.

14. The system of claim 1, wherein the memory comprises a protected storage, the protected storage comprising:

one or more storage areas;

logic for controlling access to the one or more storage areas; and

a secret.

15. The system of claim 14, wherein the one or more storage areas comprise a data storage and a code storage.

16. The system of claim 15, wherein the secret is comprised within the code storage.

17. The system of claim 1, wherein the memory further includes a secret.

18. The system of claim 1, wherein the memory comprises memory locations with a non-standard mapping, and wherein the crypto-processor includes a memory permission table that maps at least a portion of the memory, translating between a standard mapping and the non-standard mapping; and wherein the crypto-processor is configured to pass the memory transactions to the memory with the non-standard mapping.

19. The system of claim 18, wherein the crypto-processor is configured to receive memory transaction results from the memory in the non-standard mapping and to convert the non-standard mapping to the standard mapping.

20. A method of operating a computer system, the computer system including a crypto-processor, and a storage device, the method comprising:

transmitting a request for a memory transaction for a storage location in the storage device;

receiving the request for the memory transaction at the crypto-processor;

determining if the memory transaction is authorized for the storage location;

passing the request for the memory transaction to the storage device if the memory transaction is authorized for the storage location.

21. The method of claim 20, wherein passing the request for the memory transaction to the storage device if the memory transaction is authorized for the storage location comprises passing the request for the memory transaction to the storage device only if the memory transaction is authorized for the storage location.

22. The method of claim 20, wherein the crypto-processor includes a memory permission table that maps at least a portion of the storage locations in the storage device; and wherein determining if the memory transaction is authorized for the storage location comprises determining if the memory permission table includes an indication that the memory transaction at the storage location is allowed.

23. The method of claim 22, wherein the memory comprises memory locations with a non-standard mapping, the method further comprising:

translating the request for the memory transaction from a standard mapping to the non-standard mapping used by the memory.

24. The method of claim 23, further comprising:

receiving memory transaction results from the memory in the non-standard mapping; and

converting the non-standard mapping to the standard mapping.

25. The method of claim 21, wherein the computer system further comprises a bridge, a first bus coupled between the device and the bridge, and a second bus coupled between the bridge and the crypto-processor, wherein transmitting the request for the memory transaction for the storage location in the storage device further comprises:

transmitting the request for the memory transaction for the storage location in the storage device over the first bus;

receiving the request for the memory transaction for the storage location in the storage device from the first bus; and

transmitting the request for the memory transaction for the storage location in the storage device over the second bus.

26. The method of claim 21, wherein the storage device comprises a memory; wherein transmitting a request for a memory transaction for a storage location in the storage device comprises transmitting the request for the memory transaction for a memory location in the memory; wherein determining if the memory transaction is authorized for the storage location comprises determining if the memory transaction is authorized for the memory location; and wherein passing the request for the memory transaction to the storage device only if the memory transaction is authorized for the storage location comprises passing the request for the memory transaction to the memory only if the memory transaction is authorized for the memory location.

27. The method of claim 26, wherein the memory comprises a ROM; wherein transmitting the request for the memory transaction for a memory location in the memory comprises transmitting the request for the memory transaction for a memory location in the ROM; and wherein passing the request for the memory transaction to the memory only if the memory transaction is authorized for the memory location comprises passing the request for the memory transaction to the ROM only if the memory transaction is authorized for the memory location .

28. The method of claim 27, wherein the memory comprises a flash memory; wherein transmitting the request for the memory transaction for a memory location in the memory comprises transmitting the request for the memory transaction for a memory location in the flash memory; and wherein passing the request for the memory transaction to the memory only if the memory transaction is authorized for the memory location comprises passing the request for the memory transaction to the flash memory only if the memory transaction is authorized for the memory location .

29. The method of claim 21, wherein the computer system further includes a device different from the crypto-processor; and wherein transmitting the request for the memory transaction for the storage location in the storage device comprises the device initiating the request for the memory transaction for the storage location in the storage device.

30. The method of claim 29, wherein the crypto-processor includes a secret; and wherein determining if the memory transaction is authorized for the storage location comprises

demanding an authorization from the device initiating the request, wherein the authorization comprises an indication from the device of the secret.

31. The method of claim 30, wherein the indication of the secret comprises a correct response to a challenge-response authentication; and wherein demanding an authorization from the device initiating the request comprises providing a challenge to the device, and the device providing the correct response to the challenge.

32. The method of claim 31, wherein the storage device comprises a protected storage, comprising one or more storage areas, logic for controlling access to the one or more storage areas, and a secret, wherein the one or more storage areas includes the storage location; wherein transmitting the request for the memory transaction for the storage location in the storage device comprises transmitting the request for the memory transaction for the storage location in the protected storage; and wherein passing the request for the memory transaction to the storage device only if the memory transaction is authorized for the storage location comprises passing the request for the memory transaction to the protected storage only if the memory transaction is authorized for the storage location; the method further comprising:

receiving the request for the memory transaction at the logic;

verify the authorization using the logic and the secret; and

passing the request for the memory transaction an appropriate one of the one or more storage areas.

33. A system, comprising:

a first processor;

a second processor coupled to the first processor; and

a storage device operably coupled to the first processor through the second processor;

wherein the second processor is configured to control access to the storage device.

34. The system of claim 33, further comprising:

a bridge coupled between the first processor and the second processor.

35. The system of claim 34, further comprising:

a second bridge coupled between the bridge and the second processor.

36. The system of claim 35, further comprising:

a bus that couples the second bridge and the second processor, wherein the second bridge and second processor each include bus interface logic configured to master the bus.

37. The system of claim 33, wherein the second processor is a general purpose processor configured as a crypto-processor.

38. The system of claim 33, wherein the second processor is a crypto-processor.

39. The system of claim 33, wherein the storage device is a memory.

40. The system of claim 39, wherein the memory is a ROM.

41. The system of claim 39, wherein the memory is a flash memory.

42. The system of claim 33, wherein the storage device is a hard drive.

43. The system of claim 33, wherein the storage device is an optical drive.

44. The system of claim 33, wherein the storage device comprises a semiconductor storage device or a magnetic storage device.

45. The system of claim 33, wherein the second processor is further configured to understand address mapping for the memory.

46. The system of claim 33, wherein the second processor implements a challenge-response mechanism to authenticate memory accesses to the memory.

47. The system of claim 46, wherein the second processor includes:
at least one register configured to store a secret value; and
a random number generator.

48. The system of claim 47, wherein the storage device stores the secret value.

49. The system of claim 48, wherein, at boot time, the first processor is configured with the secret value, allowing the first processor to access the storage device through the second processor.

50. A method for operating a computer system, comprising a requesting device, a storage device, and a security device, wherein the requesting device is operably coupled to the storage device through the security device, the method comprising:

receiving a transaction request for a storage location associated with the storage device from the requesting device;

determining if the requesting device is authorized to access the storage device; and

mapping the storage location in the transaction request according to the address mapping of the storage device if the requesting device is authorized to access the storage device.

51. The method of claim 50, further comprising:

completing the transaction request.

52. The method of claim 50, wherein the requesting device is a processor, wherein receiving a transaction request for a storage location associated with the storage device from the requesting device comprises receiving a transaction request for a storage location associated with the storage device from the processor, wherein determining if the requesting device is authorized to access the storage device comprises determining if the processor is authorized to access the storage device, and wherein mapping the storage location in the transaction request according to the address mapping of the storage device if the requesting device is authorized to access the storage device comprises mapping the storage location in the transaction request according to the address mapping of the storage device if the processor is authorized to access the storage device.

53. The method of claim 50, wherein the storage device comprises a memory; wherein receiving a transaction request for a storage location associated with the storage device from

the requesting device comprises receiving a transaction request for a memory location associated with the memory from the requesting device; wherein determining if the requesting device is authorized to access the storage device comprises determining if the requesting device is authorized to access the memory; and wherein mapping the storage location in the transaction request according to the address mapping of the storage device if the requesting device is authorized to access the storage device comprises mapping the memory location in the transaction request according to the address mapping of the memory if the requesting device is authorized to access the memory.

54. The method of claim 50, wherein the storage device comprises a hard drive; wherein receiving a transaction request for a storage location associated with the storage device from the requesting device comprises receiving a transaction request for a storage location associated with the hard drive from the requesting device; wherein determining if the requesting device is authorized to access the storage device comprises determining if the requesting device is authorized to access the hard drive; and wherein mapping the storage location in the transaction request according to the address mapping of the storage device if the requesting device is authorized to access the storage device comprises mapping the storage location in the transaction request according to the address mapping of the hard drive if the requesting device is authorized to access the hard drive.

55. The method of claim 50, wherein determining if the requesting device is authorized to access the storage device comprises the security device determining if the requesting device is authorized to access the storage device; and wherein mapping the storage location in the transaction request according to the address mapping of the storage

device if the requesting device is authorized to access the storage device comprises the security device mapping the storage location in the transaction request according to the address mapping of the storage device if the security device determines that the requesting device is authorized to access the storage device.

56. The method of claim 55, wherein the security device is a crypto-processor; wherein the security device determining if the requesting device is authorized to access the storage device comprises the crypto-processor determining if the requesting device is authorized to access the storage device; and wherein the security device mapping the storage location in the transaction request according to the address mapping of the storage device if the security device determines that the requesting device is authorized to access the storage device comprises the crypto-processor mapping the storage location in the transaction request according to the address mapping of the storage device if the crypto-processor determines that the requesting device is authorized to access the storage device.

57. The method of claim 50, wherein determining if the requesting device is authorized to access the storage device comprises:

providing a challenge in response to receiving the transaction request;

receiving a response to the challenge; and

determining if the response to the challenge is equal to an expected response.

58. A computer system comprising:

means for storing a plurality of values;

means for controlling access to the means for storing the plurality of values;

means for requesting one or more of the plurality of values from the means for storing the plurality of values, wherein the means for controlling access to the means for storing the plurality of values is operably coupled between the means for storing a plurality of values and the means for requesting one or more of the plurality of values.

59. A computer readable program storage device encoded with instructions that, when executed by a computer system including a crypto-processor, and a storage device, performs a method of operating the computer system, the method comprising:

transmitting a request for a memory transaction for a storage location in the storage device;

receiving the request for the memory transaction at the crypto-processor;

determining if the memory transaction is authorized for the storage location;

passing the request for the memory transaction to the storage device if the memory transaction is authorized for the storage location.

60. The computer readable program storage device of claim 59, wherein passing the request for the memory transaction to the storage device if the memory transaction is authorized for the storage location comprises passing the request for the memory transaction to the storage device only if the memory transaction is authorized for the storage location.

61. The computer readable program storage device of claim 59, wherein the crypto-processor includes a memory permission table that maps at least a portion of the storage locations in the storage device; and wherein determining if the memory transaction is authorized for the storage location comprises determining if the memory permission table includes an indication that the memory transaction at the storage location is allowed.

62. The computer readable program storage device of claim 61, wherein the memory comprises memory locations with a non-standard mapping, the method further comprising:

translating the request for the memory transaction from a standard mapping to the non-standard mapping used by the memory.

63. The computer readable program storage device of claim 62, the method further comprising:

receiving memory transaction results from the memory in the non-standard mapping; and converting the non-standard mapping to the standard mapping.

64. The computer readable program storage device of claim 60, wherein the computer system further comprises a bridge, a first bus coupled between the device and the bridge, and a second bus coupled between the bridge and the crypto-processor, wherein transmitting the request for the memory transaction for the storage location in the storage device further comprises:

transmitting the request for the memory transaction for the storage location in the storage device over the first bus;

receiving the request for the memory transaction for the storage location in the storage device from the first bus; and

transmitting the request for the memory transaction for the storage location in the storage device over the second bus.

65. The computer readable program storage device of claim 60, wherein the storage device comprises a memory; wherein transmitting a request for a memory transaction for a storage location in the storage device comprises transmitting the request for the memory transaction for a memory location in the memory; wherein determining if the memory transaction is authorized for the storage location comprises determining if the memory transaction is authorized for the memory location; and wherein passing the request for the memory transaction to the storage device only if the memory transaction is authorized for the storage location comprises passing the request for the memory transaction to the memory only if the memory transaction is authorized for the memory location.

66. The computer readable program storage device of claim 65, wherein the memory comprises a ROM; wherein transmitting the request for the memory transaction for a memory location in the memory comprises transmitting the request for the memory transaction for a memory location in the ROM; and wherein passing the request for the memory transaction to the memory only if the memory transaction is authorized for the memory location comprises passing the request for the memory transaction to the ROM only if the memory transaction is authorized for the memory location .

67. The computer readable program storage device of claim 65, wherein the memory comprises a flash memory; wherein transmitting the request for the memory transaction for a memory location in the memory comprises transmitting the request for the memory transaction for a memory location in the flash memory; and wherein passing the request for the memory transaction to the memory only if the memory transaction is authorized for the memory location comprises passing the request for

the memory transaction to the flash memory only if the memory transaction is authorized for the memory location .

68. The computer readable program storage device of claim 60, wherein the computer system further includes a device different from the crypto-processor; and wherein transmitting the request for the memory transaction for the storage location in the storage device comprises the device initiating the request for the memory transaction for the storage location in the storage device.

69. The computer readable program storage device of claim 68, wherein the crypto-processor includes a secret; and wherein determining if the memory transaction is authorized for the storage location comprises demanding an authorization from the device initiating the request, wherein the authorization comprises an indication from the device of the secret.

70. The computer readable program storage device of claim 69, wherein the indication of the secret comprises a correct response to a challenge-response authentication; and wherein demanding an authorization from the device initiating the request comprises providing a challenge to the device, and the device providing the correct response to the challenge.

71. The computer readable program storage device of claim 70, wherein the storage device comprises a protected storage, comprising one or more storage areas, logic for controlling access to the one or more storage areas, and a secret, wherein the one or more storage areas includes the storage location; wherein transmitting the request for

the memory transaction for the storage location in the storage device comprises transmitting the request for the memory transaction for the storage location in the protected storage; and wherein passing the request for the memory transaction to the storage device only if the memory transaction is authorized for the storage location comprises passing the request for the memory transaction to the protected storage only if the memory transaction is authorized for the storage location; the method further comprising:

receiving the request for the memory transaction at the logic;

verify the authorization using the logic and the secret; and

passing the request for the memory transaction an appropriate one of the one or more storage areas.

72. A computer readable program storage device encoded with instructions that, when executed by a computer, performs a method of operating a computer system comprising a requesting device, a storage device, and a security device, wherein the requesting device is operably coupled to the storage device through the security device, the method comprising:

receiving a transaction request for a storage location associated with the storage device from the requesting device;

determining if the requesting device is authorized to access the storage device; and

mapping the storage location in the transaction request according to the address mapping of the storage device if the requesting device is authorized to access the storage device.

73. The computer readable program storage device of claim 72, the method further comprising:

completing the transaction request.

74. The computer readable program storage device of claim 72, wherein the requesting device is a processor, wherein receiving a transaction request for a storage location associated with the storage device from the requesting device comprises receiving a transaction request for a storage location associated with the storage device from the processor, wherein determining if the requesting device is authorized to access the storage device comprises determining if the processor is authorized to access the storage device, and wherein mapping the storage location in the transaction request according to the address mapping of the storage device if the requesting device is authorized to access the storage device comprises mapping the storage location in the transaction request according to the address mapping of the storage device if the processor is authorized to access the storage device.

75. The computer readable program storage device of claim 72, wherein the storage device comprises a memory; wherein receiving a transaction request for a storage location associated with the storage device from the requesting device comprises receiving a transaction request for a memory location associated with the memory from the requesting device; wherein determining if the requesting device is authorized to access the storage device comprises determining if the requesting device is authorized to access the memory; and wherein mapping the storage location in the transaction request according to the address mapping of the storage device if the requesting device is authorized to access the storage device comprises mapping the memory location in the transaction request according to the address mapping of the memory if the requesting device is authorized to access the memory.

76. The computer readable program storage device of claim 72, wherein the storage device comprises a hard drive; wherein receiving a transaction request for a storage location associated with the storage device from the requesting device comprises receiving a transaction request for a storage location associated with the hard drive from the requesting device; wherein determining if the requesting device is authorized to access the storage device comprises determining if the requesting device is authorized to access the hard drive; and wherein mapping the storage location in the transaction request according to the address mapping of the storage device if the requesting device is authorized to access the storage device comprises mapping the storage location in the transaction request according to the address mapping of the hard drive if the requesting device is authorized to access the hard drive.

77. The computer readable program storage device of claim 72, wherein determining if the requesting device is authorized to access the storage device comprises the security device determining if the requesting device is authorized to access the storage device; and wherein mapping the storage location in the transaction request according to the address mapping of the storage device if the requesting device is authorized to access the storage device comprises the security device mapping the storage location in the transaction request according to the address mapping of the storage device if the security device determines that the requesting device is authorized to access the storage device.

78. The computer readable program storage device of claim 77, wherein the security device is a crypto-processor; wherein the security device determining if the requesting

device is authorized to access the storage device comprises the crypto-processor determining if the requesting device is authorized to access the storage device; and wherein the security device mapping the storage location in the transaction request according to the address mapping of the storage device if the security device determines that the requesting device is authorized to access the storage device comprises the crypto-processor mapping the storage location in the transaction request according to the address mapping of the storage device if the crypto-processor determines that the requesting device is authorized to access the storage device.

79. The computer readable program storage device of claim 72, wherein determining if the requesting device is authorized to access the storage device comprises:

providing a challenge in response to receiving the transaction request;

receiving a response to the challenge; and

determining if the response to the challenge is equal to an expected response.